REQUESTING, MODIFYING, OR RESTORING A PUBLIC KEY INFRASTRUCTURE (PKI) CERTIFICATE

LMS-CP-5630
Revision: B-5

Applicant

START

Restoring? — Yes

No

Verify that minimum eligibility requirements can be satisfied (see Note 1)

Requirements satisfied? — No → END

Yes

Obtain and complete LF 21 and submit to CITSM

Objectives:
- ensure that certificates are issued only to individuals with a legitimate requirement, who have sufficiently authenticated their identity
- re-enable a disabled certificate
- change user information
- ensure that key pairs are restored only to the key pair owner or to an authenticated individual
- ensure that the Registration Authority obtains concurrence from the Center Information Technology Security Manager prior to restoring to an authenticated individual

Approval _____ Original signed on file _____
Deputy Center Director

General Information

The following records are generated by this procedure and should be maintained in accordance with CID 1440.7:
- LaRC PKI Certificate Application and Approval Request, LF 21
- LaRC PKI Certificate Key Recovery Request, LF 22

Center Information Technology Security Manager (CITSM)

Registration Authority (RA) (contractor)

Application approved? — Yes → Process Request

No

Notify applicant in writing with Cc to RA and CITSM files

END

Notify applicant of completion

New account? — No

Yes

Complete PKI Training (see Note 2)

Appear in person at RA with NASA photo ID (see Note 3)

Install PKI software on desktop (see Note 4)

To next page

END

Note 1
All LaRC civil servants need a certificate.

Individuals who are not LaRC civil servants but have a requirement for a certificate must have a LaRC civil servant sponsor.

The following requirements must be met by LaRC civil servants and LaRC-based contractors:
- Applicants must be in possession of a NASA photo ID badge
- Applicants must have a LaRC E-mail Post Office account (see LMS-CP-5519)
- Applicants' systems must satisfy a set of minimum hardware and software system requirements (see instructions for LF 21 for the web site that lists these requirements)

Any LaRC civil servant may request an additional certificate to support a process that requires the PKI encryption technology.

Note 2
PKI training is available through SATERN at https://satern.nasa.gov

Note 3
It is the responsibility of the RA to provide two pieces of information that the applicant will use for authentication to the Certificate Authority at Ames to have the certificate pushed out to the LaRC X.500 directory server.

Note 4
Questions about software installation should be directed to the ODIN helpdesk or the applicant's system administrator. ODIN supplies this software to the Center and will install it on full seats.

For applicants without a system administrator, call the CITSM for assistance.

From previous page

Applicant

Center Information Technology Security Manager (CITSM)

Obtain and complete LF 22 and submit to CITSM (see Notes 5 & 6)

Verify the legitimacy of the request

Request approved?

No

Yes

Retain copy of LF 22 in CITSM files

Appear in person at RA to provide proof of identity

Give the reason for denial of request in writing to the applicant and retain a copy in CITSM files

END

Note 5
An applicant may request recovery of a personal key pair if:
-the password has been forgotten
-the keys have been compromised
-a compromise is suspected
-a PKI profile has been lost or damaged
-a security token has been lost or damaged

An applicant may request key recovery, with or without the key pair owner's consent if:
-the owner has left the organization and management needs to recover and decrypt files
-the owner's actions are in question by line management, the LaRC Chief Information Officer, or Center Information Technology Security Manager
-the owner's actions are in question by an external law enforcement agency or the Security & Program Protection Services

Note 6
For information on Key Recovery, refer to "What You Need to Know About Key Recovery" on LF 22.

Note 7
When a request is made without the consent of the user, the applicant must provide information on which of the user's files need to be reviewed. The user may or may not be notified of the action depending on circumstances.

If the recovery is for reasons other than business continuity, the recovery is classified as an IT security incident and will be handled at the discretion of the CITSM.

Registration Authority (RA) (contractor)

Process Request

Sign to acknowledge receipt of key pair (see Note 7)

Notify applicant and CITSM that action is complete

Record completion on LF 22

END